

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended): ~~A security apparatus~~ An access point device for a
2 wireless LAN ~~for isolating an end station from a plurality of end stations to support~~[[ing]]
3 segregation of network traffic ~~among~~ between the end station and the plurality of end stations,
4 ~~comprising~~ the access point device serving as a common access point for communication in the
5 wireless LAN, the access point device configured to:
6 a ~~Public Access Point (PAP) component for providing a plurality of virtual Basic~~
7 ~~Service Sets (BSSs), said PAP component configured to allow any one end station among said~~
8 ~~end stations to cause creation of a virtual BSS;~~
9 receive a request from said end station that is an association request or a probe
10 request; and
11 process said request by:
12 determining for said request a basic service set (BSS) that is unknown to
13 said access point device at the time of receipt of said request by said access point device;
14 receiving at least one parameter defining said BSS;
15 establishing said BSS based at least on said at least one parameter; and
16 sending a response to said end station that includes a BSSID of said
17 established BSS,
18 ~~wherein any number of said end stations can belong to said virtual BSS;~~
19 ~~wherein said PAP appears to said end stations as multiple physical access points,~~
20 ~~one access point for each of said virtual BSSs.~~

1 2. (Currently amended): The ~~apparatus~~ access point device of Claim 1, ~~said~~
2 ~~PAP provisioning~~ further configured to provision a plurality of separate LAN segments while
3 providing separate link privacy and integrity for each of said LAN segments.

3. (Canceled)

4. (Currently amended): The ~~apparatus~~ access point device of Claim 1,
further comprising:
a plurality of PAPs; and
a location-update protocol for updating forwarding tables of bridges that connect
said PAPs together other access points.

5. (Currently amended): The ~~apparatus~~ access point device of Claim 1,
further comprising:
a fine bridging method for limiting communications between said end stations
that belong to said ~~virtual~~ established BSS.

6. (Canceled)

7. (Currently amended): A method in an access point device for a secure
wireless network to support segregation of network traffic among a plurality of stations, each of
said stations having a hardware (MAC) address, comprising:
receiving an association request or a probe request from a first station;
determining for said request a basic service set (BSS) that is unknown to said
access point device at the time said request was received by said access point device;
receiving at least one parameter which defines said BSS;
establishing said BSS based at least on said at least one parameter, thereby
creating a ~~virtual~~ 802.11 Basic Service Set (BSS) for a subset of said stations, ~~wherein the~~
~~step of creating can be initiated by any station in said subset; and~~
sending a response to said end station that includes a BSSID of said created BSS,
wherein stations in said subset belong to said ~~virtual~~ created BSS and share a
group security association.

8-21. (Canceled)

1 22. (Currently amended): The access point device method of Claim [[7]]1,
2 wherein said end station is a member of a Class-1 BSS or a Class-3 BSS at said access point
3 device, said virtual BSS comprising any of:
4 a Class-1 and a Class-3 virtual BSS;
5 wherein a PAP supports exactly one Class-1 virtual BSS and one or more multiple
6 Class-3 virtual BSSs;
7 wherein a Class-1 virtual BSS is the only virtual BSS which a station is allowed
8 to occupy while it is in 802.11 State 1 or 2, as governed by said PAP;
9 wherein when in State 3, a station is allowed to join a Class-3 virtual BSS; and
10 wherein a Class-3 virtual BSS is determined by the kind of authentication
11 used to authenticate said station.

1 23. (Currently amended): The access point device method of Claim 22,
2 wherein a Class-1 ~~virtual~~ BSSID is the BSSID field of every Class 1 and Class 2 frame that has
3 such a field, and wherein a Class-3 BSSID is the BSSID field of every Class 3 frame that has
4 such a field.

1 24. (Currently amended): The access point device method of Claim 22,
2 wherein a Class-1 ~~virtual~~ BSSID is the receiver or transmitter address field, where appropriate,
3 for Class 1 and Class 2 frames, and wherein a Class-3 BSSID is the receiver or transmitter
4 address field, where appropriate, for Class 3 frames.

25. (Canceled)

1 26. (Currently amended): The access point device method of Claim [[22]]1,
2 wherein said PAP does not have to beacon for a Class-3 virtual BSS if it does not support Power-
3 Save (PS) mode for end stations in that BSS;

4 wherein if said ~~PAP~~does access point device beacons for said established BSS-a
5 ~~Class 3 BSS~~, then an SSID element in every beacon specifies a broadcast SSID or an SSID for
6 said established BSS;

7 wherein a ~~Class 3 virtual BSS~~ is prevented from being identified through
8 beaoning.

27-35. (Canceled)

1 36. (Currently amended): The access point device method of Claim [[35]]55,
2 wherein ~~said received MPDU~~an MPDU received from said DSM or said WM is also relayed to
3 said DSM if [[said]]a destination address ~~thereof~~(Address 3 field of MPDU) is an address of an
4 end station that is not associated with said ~~PAP~~access point device; or

5 if said destination address is a group address;

6 wherein said MPDU relayed to said DSM has a VLAN tag if said [[DS]]DSM is
7 VLAN aware, and is untagged otherwise; and

8 wherein said VLAN tag is a pre-image of ~~said Address 4~~a source address field of
9 said received MPDU under said [[PAP's]] DSM VLAN mapping.

37. (Canceled)

1 38. (Currently amended): The access point device method of Claim [[37]]1,
2 wherein ~~said encryption process used by said PAP~~ before sending an 802.11 Data or
3 Management frame to said end station, said access point device is configured to WM ~~comprises a~~
4 ~~mechanism that perform~~[[s]] the steps of:

5 identifying a security association for said frame; and

6 [[then]] using said security association to construct an expanded frame for
7 transmission according to an encipherment and authentication code protocol.

1 39. (Currently amended): The access point device method of Claim 38,
2 wherein if a frame destination address (~~Address 1 field~~) is the address of [[a]]said end station
3 then a ~~unicast~~-security association shared between ~~that said end station~~ and said PAP-access
4 point device is used in said frame expansion; and
5 wherein if said frame is a Data frame and its destination address is a group
6 address then said ~~MPDU bridge protocol~~access point device identifies a destination virtual-BSS
7 for said frame, wherein a group security association for said identified-virtual-destination BSS is
8 used in said frame expansion.

1 40. (Currently amended): The access point device method of Claim 39,
2 wherein ~~a non-PAP~~said end station transmits an 802.11 MPDU of type Data or Management ~~to~~
3 ~~said DSM~~ using a ~~unicast~~-security association ~~it that said end station~~ shares with said access
4 point device~~PAP~~ in its virtual-BSS.

1 41. (Currently amended): The access point device method of Claim 40,
2 wherein when receiving an 802.11 Data or Management frame from said ~~end station-WM~~, said
3 PAP-access point device attempts to decipher and verify integrity of said frame using a ~~unicast~~
4 security association for ~~a-an end~~ station identified by a source address field (Address 2 field) of
5 said MPDU.

1 42. (Currently amended): The access point device method of Claim 41,
2 wherein when receiving an 802.11 MPDU of type Data or Management from said access point
3 device~~PAP~~, ~~a non-PAP~~said end station attempts to decipher and verify integrity of said frame by
4 using a ~~unicast~~-security association ~~it that said end station~~ shares with said access point device
5 PAP-if a destination address of said frame (~~Address 1 field~~) is an address of said end station, and
6 by using a group security association ~~of its Class 3 virtual-BSS~~-if said destination address of said
7 frame is a group address.

43. (Previously presented): A location-update method for updating forwarding tables of bridges, or other interconnection media, that connect Public Access Points (PAPs) together, where multiple PAPs are attached to different bridges in a spanning tree of a bridged LAN and an end station associates with one of said PAPs and then reassociates with a new PAP, comprising steps of:

said new PAP sending a directed Bridge Protocol Data Unit (BPDU) to said PAP with which said station was previously associated;

wherein destination address of said BPDU is current access point (AP) address of a Reassociation Request frame, which is a Class-3 virtual BSS identifier (BSSID); and

wherein source address is a hardware address of said station;

upon receiving a relocation MPDU at a particular port, a bridge updating its forwarding table with an entry that binds a receiving port to a source address of said MPDU; and

said receiving bridge forwarding a relocation MPDU to its designated root port, unless said MPDU arrived on that port or said receiving bridge is a root of said spanning tree;

wherein if said MPDU is received at said designated root port of said bridge or by a root bridge then it is forwarded according to a learned forwarding table of said bridge, which optionally comprises flooding said MPDU to all ports except said receiving port.

44. (Previously presented): A fine bridging method for a wireless network, comprising steps of:

decoupling identification of a broadcast or multicast domain with a Basic Service Set (BSS); and

determining bridging behavior of an access point (AP) by a policy expressed as a directed graph;

wherein for a given policy, a broadcast domain for a node is itself and all nodes it must access;

wherein said broadcast domain set of said policy is a set of broadcast domains for its nodes; and

11 wherein nodes of said graph are stations and there is an edge from a first station to
12 a second station if and only if said first station must be able to communicate with, or access said
13 second station, such that said second station must be able to receive directed or group frames
14 from said first station.

1 45. (Original): The method of Claim 43, further comprising the step of:
2 providing a group security association per broadcast domain.

1 46. (Original): The method of Claim 45, wherein each station (node)
2 possesses a first group security association of a broadcast domain for itself in said policy, and a
3 second set of group security associations, one for every other broadcast domain in said policy of
4 which said station is a member.

1 47. (Original): The method of Claim 46, wherein said first group security
2 association is used by said station for sending group frames and said second set of group security
3 associations is used for receiving group frames.

1 48. (Currently amended): The ~~access point device method~~ of Claim 42,
2 wherein broadcast and multicast traffic in different ~~virtual~~ basic service sets is protected with
3 different encipherment or authentication-code protocols in said network.

1 49. (Currently amended): The ~~access point device method~~ of Claim 42,
2 wherein ~~unicast traffic between a PAP and a said access point device and said end station use~~
3 encipherment or authentication-code protocols that are different from encipherment or
4 authentication-code protocols used for traffic ~~and~~ between said access point device PAP and
5 another end station that is associated with another BSS that is established in said access point
6 device ~~in a virtual BSS is protected with different encipherment or authentication-code protocols~~
7 ~~in said virtual BSS.~~

50. (Canceled)

1 51. (New): The access point device of Claim 1 wherein said at least one
2 parameter is provided by said end station.

1 52. (New): The access point device of Claim 1 wherein said at least one
2 parameter is provided by a source other than said end station.

1 53. (New): The access point device of Claim 1 wherein said request includes
2 an SSID (service set identifier), wherein said at least one parameter is based on said SSID.

1 54. (New): The access point device of Claim 1 wherein said request is for a
2 Class-1 virtual BSS.

1 55. (New): The access point device of Claim 22,
2 wherein said access point device implements a MAC Protocol Data Unit (MPDU)
3 bridge protocol,
4 wherein a plurality of BSS's including said established BSS are known to said
5 access point device,

6 (A) wherein for an MPDU which has a null VLAN tag or is absent a VLAN tag
7 and which has been received from a distribution system medium (DSM), said MPDU is relayed
8 to one of said BSS's when either:

9 (1) a destination address of said MPDU is an address of an end station
10 which belongs to said one of said BSS's and which is associated with said access point
11 device; or

12 (2) said destination address is a group address, said one of said BSS's has
13 an end station which belongs to a group identified by said group address and which is
14 associated with said access point device,

15 wherein an address for relaying said MPDU to said one of said BSS's is
16 based on a BSSID thereof,

(B) wherein for an MPDU which has a non-null VLAN tag and which has been received from a DSM, then:

(1) said MPDU is relayed to said one of said BSS's that is identified by a BSSID to which said non-null VLAN tag is mapped according to a DSM VLAN mapping of said access point device, wherein an address for relaying said MPDU is based on a BSSID of said identified BSS; and

(2) said MPDU is not relayed if a DSM VLAN mapping is undefined for said non-null VLAN tag,

(C) wherein for an MPDU which is received from a wireless medium (WM), said MPDU is relayed to one of said BSS's identified by a source address field of said MPDU when said destination address of said MPDU is an address of an end station which belongs to said identified BSS and which is associated with said access point device or when said destination address is a group address.